FISMA / Certification & Accreditation
What is it and Why it is important to you?

Frank Husson

Director, Cyber Security Division

Office of the Associate CIO for Enterprise Operations

US Department of Energy
Office of the Chief Information Officer

Agenda

- **Introduction –** Frank Husson, Director, Cyber Security Division
  - **DOE HQ C&A Overview**
    - Current Convention
    - Enclave Convention
  - **OCIO Enclave Hierarchy**
  - **C&A Convention Comparison**
  - **Summary**
- **NIST –** Dr. Ron Ross, Manager, NIST Computer Security Division
  - **Managing Enterprise Risk**
    - **FISMA Lessons Learned & Implementation Tips**

Current Convention and Inventory

C&A Package

1. System Security Plan
2. Privacy Impact Assessment
3. Configuration Management Plan
4. Contingency Plan
5. Interconnection Security Agreements, MOU/MOA
6. Risk Assessment
7. Security Test & Evaluation Plan
8. Security T&E Test Report
9. Plan of Action and Milestones
10. Certification Recommendation Letter
11. Security Assessment Report

Systems Inventory

General Support Systems (10)
- Oracle
- Linux
- Solaris
- Windows
- NAS
- IBM AIX
- IBM Enterprise Server
- HP MPE
- DOECOE
- DOEnet

Major Applications (6)
- Applix
- ePortal
- iPortal
- PCA/PKI
- Email Support Services
- Energy.gov

Total Package Inventory - 16

Enclave Convention

Enclave Approach - Overview

- Facilitates logical grouping & consolidation of systems
- Leverages Common Security Controls
- Precise System Boundaries

Benefits

- ***Significantly*** lowers redundancy in C&A package documentation for each GSS or MA
- ***Substantially*** reduces C&A "Level of Effort" for System Owners
- ***Meets*** National Institute Standards & Technology (NIST) and DOE requirements for C&A

OCIO Enclave Hierarchy

Major Applications

Hosted
- Applix, ePortal, iPortal
- Email Support Services, Energy.gov

Housed
- PCA/PKI

AHE

General Support Systems:
- Oracle, Linux, Solaris, Windows, NAS
- IBM AIX, IBM Enterprise Server, HP MPE

DOECOE

General Support Systems:
- DOECOE Desktop

Networks

- DOEnet (GSS) - WAN, HQ Data Network MAN/LAN, Remote Access, Internet Access

Network Enclave Template

Description of Network Enclave

- **Network Infrastructure Components**
  - WAN
  - HQ Data Network - MAN/LAN
  - Remote Access
  - Internet Access

Common Security Controls

- Cyber Security Program Plan
- Contingency Plan
- Configuration Management Plan
- Incident Response Plan
- Security Awareness and Training Plan
- Physical & Environmental Security
- Media Protection
- Vulnerability Scanning
- Technical controls

Security Test & Evaluation Plan (Common Security Controls)

Security Test & Evaluation Test Report

Certification Recommendation Letter

Appendix – Network Infrastructure

- Risk Assessment
- System Security Plan
- Security Test and Evaluation – Plan & results
- Security Test and Evaluation – Report
- Security Assessment Report
- Plan of Action and Milestones
- Memorandum of Understanding/Agreement
- Privacy Impact Assessment
- Accreditation Decision Letter

C&A Convention Comparison

Current Convention

1. RA
2. SSP
3. ST&E Plan
4. POA&M
5. PIA
6. MOA/MOU
7. Security Assessment Report
8. Certification Recommendation Letter
9. Accreditation Decision Letter
10. **Configuration Mgt. Plan**
11. **Contingency Plan**
12. **Cyber Security Program Plan**
13. **Incident Response Plan**
14. **Security Training & Awareness**
15. **Personnel Security**
16. **Environmental Security**
17. **Physical Security**
18. **Rules of Behavior**

GSS – 10
MA – (5) housed
MA – (1) hosted
Total C&A Package - 16

Enclave Convention

1. Description of Enclave and Platforms
2. Common Security Controls
3. Security T&E Plan
4. Security T&E Test Report
5. Certification Recommendation Letter
6. Accreditation Decision Letter
7. Appendix (by Platform/Major App.)
   a. Risk Assessment
   b. System Security Plan
   c. Security Test & Evaluation
   d. Plan of Action & Milestones
   e. Memorandum of Agreement
   f. Privacy Impact Assessment

GSS – 3
MA – (1) housed
MA - (1) hosted
Total C&A Packages - 5

Take-Away Points

1. Pilot/Proof of Concept - Network Enclave

2. Leverages Common Security Controls
   - GSS
   - Major Applications (hosted)

3. Benefits
   - C&A packages reduction (i.e., 16 to 5)
   - Substantially reduce documentation volume